

РОЗРОБКА ANDROID ДОДАТКІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ GOOGLE PLAY PROTECT ТА SAFETYNET VERIFY APPS API

*магістр О.В. Філоненко, канд. фіз.-мат. наук, доц. О.П. Черних, доц.
О.М. Шейн, Національний технічний університет "Харківський
політехнічний інститут", м. Харків*

У теперішній час ринок мобільних додатків є одним з найпоширеніших. Він містить в собі як якісні екземпляри, так і погані, а іноді навіть шкідливі. Найпопулярнішими мобільними операційними системами у наш час є iOS та Android. У першому кварталі 2017 року система Android була найпоширенішою у світі. Тому розробка додатків під цю операційну систему є дуже актуальною.

Одним із способів встановлення нового додатку до смартфона на базі Android є скачування та установка його за допомогою Google Play Market. Проте, не завжди користувачі встановлюють додатки із перевірених джерел, частіше завантажують із шкідливих ресурсів. У даній роботі запропоновано спосіб перевірки на шкідливість вже встановлених на пристрої додатків.

Для вирішення проблеми було обрано технологію Google Play Protect, яка містить в собі захисний механізм Verify App та мову програмування Java. Verify App – це набір декількох API-інтерфейсів, які дають змогу розробникові захистити додаток від встановленого потенційно небезпечного програмного забезпечення. Проте, корисним для поставленої задачі є саме Verify Apps API. Серед представлених API є наступні:

`isVerifyAppsEnabled` – останні дії, які користувач виконував із функцією VerifyApps;

`enableVerifyApps` – метод, який запрошує дозволу у користувача для застосування VerifyApps та повертає об'єкт, який містить останні активності користувача із даною функцією;

`listHarmfulApps` – метод отримання списку потенційно-небезпечних додатків, які встановлено на користувацькому пристрої.

Для розробника технологія Google Play Protect дає змогу створювати якісні та захищені додатки, які можуть використовуватись на підприємствах для захисту своїх внутрішніх даних. Це не тільки дозволяє зберегти комерційну таємницю, а і зекономити на відновленні втраченої інформації та репутації компанії.